ACCESS CHAIN TRACING SYSTEM, NETWORK SYSTEM, AND STORAGE MEDIUM

Abstract

Log data for a packet that is exchanged across a network are recorded in a log box. At this time, the data size of the packet and the detection time are recorded. When an illegal access has occurred at a target computer, the tracing of an access chain is performed on the log information. The tracing of the access chain is performed as follows. A change in the size of the data in a packet in accordance with the time of the first connection, and a change in the size of the data in a packet in accordance with the time of the second connection are calculated using the log data, and then the shapes of the graphs formed by these packet series are compared. When the shapes of the graphs are similar, it is ascertained that the pertinent connections are included in the same chain.